

W 5487/01-US

W 5488/01-JP

Claims

1. Procedure for the protection of computer software and/or computer-readable data against unauthorized use, including the steps
 - encoding of software or data by the licensor dependent on license parameters containing a Firm Code (FC) assigned to the licensor and a User Code (UC) allocated by the licensor of the software or the data, which together initiate the encoding;
 - storage of the encoded software or data on a data medium of the licensee;
 - encoded transmission of the license parameters from the licensor to the licensee;
 - storage of the license parameters in a nonvolatile memory of the licensee;
 - automatic decoding of the software or data by means of a decoder dependent on the storage license parameters during the use of the software or data by the licensee;
 characterized in that
 - the encoding of the software or data is initialized dependent on a secret Firm Key (FK) freely selected by the licensor;
 - the encoding of the transmission of the license parameters occurs dependent on a secret Private Serial Key (SK);
 - the decoding of the software or data is initialized dependent on the Firm Key (FK) selected by the licensor.
2. Procedure in accordance with Claim 1, characterized in that the secret Private Serial Key (SK) is produced randomly at the licensee without the licensee, the licensor, or anyone else being able to influence that.
3. Procedure in accordance with Claim 1 or 2, characterized in that the signature of the transmission of the license parameters from the licensor to the licensee occurs dependent on a unique Serial Number (SN) firmly assigned to the licensee.
4. Procedure in accordance with one of Claims 1-3, characterized in that
 - the licensor is assigned a secret Firm Common Key (FCK), which is produced from a Common Key (CK) through encoding dependent on the Firm Code (FC) of the licensor;
 - the installation, changing, or deletion of the license parameters occurs dependent on the Firm Common Key (FCK).
5. Procedure in accordance with one of Claims 1-4, characterized in that the storage of the license parameters occurs within a protective device (3) developed as a hardware supplement.

6. Procedure in accordance with Claim 5, characterized in that the automatic decoding of the protected software or data occurs by means of an encoder and decoder (7) arranged within the protective device (3).

7. Procedure in accordance with Claim 5 or 6, characterized in that the protective device (3) contains a limiter (9) secure against manipulation that limits the time period and/or the number of decodings of the protected software or data.

8. Procedure in accordance with one of Claims 5-7, characterized in that
 -- a secret Private Box Key (BK) determined by the producer is stored in the protective device (3);

-- the encoding of the transmission of license parameters between the licensor and the licensee occurs dependent on this Private Box Key (BK).

9. Protective device for use in the procedure in accordance with Claim 1, with
 -- an interface (4) for connection with the computer (2) of the licensee;
 -- a microprocessor (5);
 -- a nonvolatile memory (6) in which the license parameters are stored;
 -- an encoder and decoder (7) for the automatic decoding of the software or data dependent on the stored license parameters;
 characterized by
 -- an installation (8) for the production of a random secret Private Serial Key (SK) for the encoding of the transmission of the license parameters between the licensor and licensee.

10. Protective device in accordance with Claim 9, characterized in that the memory (6) includes several memory areas (6a, 6b, 6c) for the storage of license parameters of different licensors.

11. Protective device in accordance with Claim 9 or 10, characterized in that the microprocessor (5), the memory (6), the encoder/decoder (7), and the installation (8) for the production of the Private Serial Key (SK) are developed on a single integrated semiconductor circuit (ASIC).

12. Protective device in accordance with one of Claims 9-11, characterized in that it contains a limiter (9) secure from manipulation that limits the time period and/or the number of decodings of the protected software or data.